OFFICIAL RESPONSES TO VENDOR QUESTIONS
RFP-2018-OMS-01-MEDIC

No.	Question	Answer
1.	Appendix G, A.4: NIST covers a very large range of standards from a wide array of services. Are there specific standards DHHS would like vendors to use?	The State's information security policies and procedures are based on the NIST SP 800 series that describe information technology security policies, procedures and guidelines. Specifically, the NIST SP 800-53, Appendix F "Security and Privacy Controls for Federal Information Systems and Organizations" provides the risk management framework that should be followed by any state service provider.
2.	Appendix G, A.4: Q1) How are vendors to provide certification of NIST requirements? Q2) Does DHHS require vendors to have NIST issue the certification?	Q1 – How are vendors to provide certification of NIST requirements? The State requires an attestation that the vendor has followed the NIST SP800 series in developing its information technology policies and procedures. The vendor's annual security assessment which is required under Appendix G, A2 can serve as this attestation as long as the third party includes a review of the vendor's policies, procedures and guideline as part of its assessment. Q2 – Does DHHS require vendors to have NIST issue the certification? No, DHHS does not require NIST to issue the certification.
3.	Appendix G, A.4: How are vendors to provide certification of OWASP requirements? According to OWASP's site, OWASP does not offer any certifications. https://www.owasp.org/index.php/OWASP_Certification	The State requires an attestation that any application provided by the vendor has been appropriately hardened to prevent exploitation by the common coding vulnerabilities as identified by the latest version of the OWASP Top 10. The vendor's annual security assessment which is required under Appendix G, A2 can serve as this attestation as long as the third party independent assessor includes a review of the application to include common vulnerabilities
4.	Appendix G, A.8: What mechanism(s) will the State's Chief Information Officer use for detection of security vulnerabilities?	The State reserves the right to use a variety of automated or manual processes for detection of security vulnerabilities in the vendor's environment. Any effort will be a cooperative effort between the State and the vendor and will include a determination, based on the events at that time, about the scope of the detection effort as well as the appropriate rules of engagement.